AMENDMENTS TO THE DRAWINGS

Please replace FIGS. 1-5 with the replacement drawings FIGS. 1-5 attached hereto.

**Attachment: Replacement Sheets (FIGS. 1-5)**

**REMARKS**

Applicant submits herewith formal drawings for FIGS. 1-5 to replace the originally filed drawings.

The Examiner rejected claims 1, 2, 4-10, 22-25, 46 and 56-71 under 35 U.S.C. §103(a) as being unpatentable over RFC 3325 Internet Draft (authored by Jennings and Peterson) in view of the reference "draft-ietf-sip-privacy-04.txt" by Marshall *et al.*, and further in view of "3GPP TSG SA WG3 Security - S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces" (hereinafter "3GPP"). The Examiner rejected claim 13 under 35 U.S.C. §103(a) as being unpatentable over Jennings in view of Marshall, and further in view of RFC 3574 by Soininen.

Applicant amended independent claim 1 to clarify that the second layer indication included with the modified message is an indication that the message has not been through a security check at the first layer prior to being received at the first network. Support for the clarification is provided throughout the application, including, for example, at page 4, paragraphs 53-55 of the published application (US 2004/0177145). Applicant similarly amended independent claims 22, 25 and 46.

Applicant's independent claim 1 recites "a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check at the first layer prior to being received at the first network when the result of the determination is that the message has not been through a security check, wherein the second layer is a higher layer than the first layer." Thus, an indication included with the modified message indicates that the message has not been through a security check at the first layer (e.g., a security check performed by a Za interface) prior to being received at the network (i.e., the indication indicates that a security check outside the first network has not been performed):

> [0053] The first embodiment is represented by the steps in FIGS. 2a and 2b. Turning firstly to FIG. 2a, at the start of the process (30) a SIP message is received at the I-CSCF. This message could either have been received over the Za interface or directly from outside the network. In step 32, the I-CSCF 2 determines which of these two alternatives is the case.

> [0054] If the answer is no (i.e. message not received via Za interface), the I-CSCF 2 proceeds to step 34 at which a modification is made to the P-Asserted-Identity header of the message. In this embodiment a parameter is added to the header to indicate that the message has not been through security clearance. The example header shown above is therefore modified to have the following format:
>
> [0055] <sip:user1_public1@home1.net>;screening=no
>
> (US 2004/0177145, FIGS. 2a and 2b, and page 4, paragraphs 53-55)

In rejecting claim 1, the Examiner admitted that "Jennings shows when a message *will* not go through a security check, then modifying the message (pg. 6, paragraph 1) but does not show modifying when a message *has not been* through a security check" (Emphasis in the original, Office Action, page 3). It follows, therefore, that Jennings also fails to disclose "a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check at the first layer prior to being received at the first network," as recited in independent claim 1.

Marshall described "extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy" (Marshall, Abstract). Marshall explains that when a message from an untrusted entity is received by a proxy, the proxy examines if the message includes Remote-Party-ID header. If the message includes a Remote-Party-ID header, the Proxy has to verify the information in the header. If the verification is successful, the proxy adds an "rpi-screen" parameter that is set to "yes", and if the verification fails, the proxy adds an "rpi-screen" parameter that is set to "no":

> 7.5 Proxy Behavior
>
> When a proxy supporting this extension receives an INVITE, OPTIONS,
> REGISTER or extension method request from a trusted entity, it does not apply any special processing until the message is forwarded to the next hop. If the message instead came from an untrusted entity, the proxy MUST do the following:

> First, the proxy MUST examine the message for the presence of any Remote-Party-ID headers. Since the request was received from an untrusted entity, each of these MUST either be verified by the proxy or have their rpi-screen parameter set to "no". If the proxy is able to successfully verify the information in a Remote-Party-ID header field (by means outside the scope of this document), the proxy MUST add an rpi-screen parameter set to "yes" for that Remote-Party-ID. Furthermore, this MUST be the only rpi-screen parameter for that Remote-Party-ID. If verification fails however, further processing depends on the reason for the failure. Two different failure reasons are defined here:
>
> * The information provided could not be verified because the proxy does not support verification of the identity information for this particular Remote-Party-ID.
>
> * The proxy supports verification of this particular Remote-Party-ID, however the identity information provided is incorrect and the proxy detected that, or the identity information could not be verified.
>
> In the first case, the proxy MUST add an rpi-screen parameter set to "no". The proxy SHOULD furthermore ensure this is the only rpi-screen parameter. In the second case, the proxy MUST by default add an rpi-screen parameter set to "no" and ensure this is the only rpi-screen parameter, however individual extensions and local procedures MAY specify a different behavior, for example rewrite or removal of the offending Remote-Party-ID header field.
>
> (Marshall, Section 7.5)

Thus, Marshall's proxy adds an "rpi-screen" parameter to indicate whether a verification check (which the Examiner presumably equated to claim 1's security check) that the proxy performed has been successful. In other words, the indication added to Marshall's message pertains to a verification check performed at the proxy after the proxy has received the message. This added indication, therefore, is not an indication of whether the message has been at a security check at the first layer prior to being received at the proxy. Accordingly, Marshall fails to disclose or suggest at least the features of "a modifier configured to modify the message so as to include a second

layer indication that the message has not been through a security check at the first layer prior to being received at the first network," as recited in independent claim 1.

3GPP fails to cure the deficiencies of the teachings of Marshall and/or Jennings as they relate to the features pertaining to adding an indication that a message has not been through a security check at a first layer prior to being received at a first network. Accordingly, 3GPP too fails to disclose or suggest at least the features of "a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check at the first layer prior to being received at the first network," as recited in independent claim 1.

Because none of the references discloses or suggests, alone or in combination, at least the features of "a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check at the first layer prior to being received at the first network," Applicant's independent claim 1, and the claims depending from it, are patentable over the cited art.

Applicant's independent claims 22, 25 and 46 recite "when the result of the determination is that the message has not been through a security check modify the message so as to include a second layer indication that the message has not been through a security check at the first layer prior to being received at the security server," or similar language. For reasons similar to those provided with respect to independent claim 1, independent claims 22, 25 and 46, and the respective claims depending from them, are patentable over the cited art.

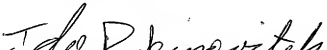
## CONCLUSION

On the basis of the foregoing amendments, the pending claims are in condition for allowance. It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper. Applicant asks that all claims be allowed.

If there are any questions regarding these amendments and remarks, the Examiner is encouraged to contact the undersigned at the telephone number provided below. The Commissioner is hereby authorized to charge any additional fees that may be due, or credit any overpayment of same, to Deposit Account No. 50-0311, reference No. 39700-591001US.

Respectfully submitted,

Date: November 12, 2009



Ido Rabinovitch
Reg. No. L0080

Address all written correspondence to
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
One Financial Center
Boston, Massachusetts 02111
**Customer No. 64046**
Telephone: 617-348-1806
Facsimile: 617-542-2241